185 Franklin Street, 13th Floor
Boston, MA 02110
Tel (617) 743-2445
Fax (617) 737-0648

Bruce P. Beausejour
Vice President and General Counsel New England

March 18, 2003

BY HAND DELIVERY

Mary L. Cottrell, Secretary
Department of Telecommunications and Energy
Commonwealth of Massachusetts
One South Station, 2nd Floor
Boston, MA 02110

Re: Performance Assurance Plan – Service Waiver Request

Dear Secretary Cottrell:

Enclosed please find an original and five copies of the Petition of Verizon Massachusetts for a Waiver of Certain Service Results Measured Under the Performance Assurance Plan ("PAP") for January 2003. An electronic copy of the Petition has been served on all parties. Exhibit 2 to the Petition contains confidential CLEC information that is being provided only to the Department. CLEC-specific reports will be provided upon request.

Appendix D of the PAP outlines the requirements for submitting a waiver and includes an illustrative timeline. In order to meet the May 1, 2003 due date for the processing of January credits, the Department's ruling on this waiver should be issued by April 18th.

Respectfully submitted,

Bruce P. Beausejour

Attachments

cc: Attached Service List (e-mail)

PETITION OF VERIZON MASSACHUSETTS FOR A WAIVER OF CERTAIN SERVICE QUALITY RESULTS MEASURED UNDER THE PERFORMANCE ASSURANCE PLAN FOR JANUARY 2003

Bruce P. Beausejour
185 Franklin Street
Boston, MA 02110
(617) 743-2445

Counsel to
Verizon Massachusetts

Dated: March 18, 2003

TABLE OF CONTENTS

EXHIBITS

PETITION OF VERIZON MASSACHUSETTS INC. FOR A WAIVER OF CERTAIN SERVICE QUALITY RESULTS MEASURED UNDER THE PERFORMANCE ASSURANCE PLAN FOR JANUARY 2003

Verizon Massachusetts ("Verizon MA") requests that the Department waive certain service performance results for January 2003 that would otherwise be included in the calculation of monthly bill credits due to Competitive Local Exchange Carriers ("CLECs") under provisions of the Performance Assurance Plan ("PAP"). Certain systems employed by Verizon MA and its affiliated Operating Telephone Companies ("OTCs") (collectively, "Verizon") were subject to an Internet computer attack by a "worm" during the weekend of January 25, 2003 (the "Slammer Worm"). Section II(J) of the PAP provides that Verizon MA may file for a waiver of service results when there is a situation that is beyond its control "that negatively affect[s] its ability to satisfy only those measures with absolute standards." (PAP at 22.)[1] This extraordinary event, which was beyond Verizon MA's control, prevented it from satisfying three of the PAP's pre-order wholesale measures with absolute standards during January 2003.[2] None of the parity metrics were affected.

Verizon MA estimates that if the instant waiver request is granted, the amount of monthly credits due to CLECs will be eliminated (the filed credits were approximately $164,000). Attached hereto as Exhibit 1 is a copy of the "Performance Assurance Plan – January 2003 Monthly Report" that Verizon MA filed with the Department on February 25, 2003. Exhibit 2 contains the adjusted January 2003

---

1 Similar waiver petitions are being filed with state commissions in the Verizon East region that have adopted and effective PAPs based on the Verizon New York PAP.

2 The PO-2-02 pre-order availability metrics were affected by the Slammer Worm.

Monthly Report, which reflects the modifications that should be made to the January 2003 Monthly Report to offset the effects of the Slammer Worm on the three pre-order metrics with absolute standards. Exhibit 2 contains both the Public (aggregate) and Confidential (CLEC-specific) reports.[3]

For the reasons set forth below, the Department should grant the waiver request and allow Verizon MA to exclude the effects of the Slammer Worm for the monthly service results that will comprise the performance levels against which it will be measured under the PAP for January 2003.

I. THE SLAMMER WORM

A. THE EVENT

On January 25, 2003, at 12:30 AM Eastern Standard Time ("EST") corporate networks and the Internet began being flooded with vast quantities of traffic. One industry report estimates that "more than 90 percent of vulnerable computers [were infected] within 10 minutes." *See* CNET News.com, "Week in Review: Worms Wrath", Feb. 7, 2003. The source of the runaway traffic was traced to a worm called the SQL Slammer, also known as W32.Slammer and Sapphire (referred to herein as the Slammer Worm), which is self-propagating malicious code that exploits vulnerabilities in Microsoft SQL Server 2000, and certain other Microsoft products. The Slammer Worm crafts packets of 376 bytes and sends them to randomly chosen IP addresses on a specific port, in this case port 1434/udp.[4] The Slammer Worm targets systems running MS SQL Server 2000 and potentially affects systems running Microsoft Desktop Engine ("MSDE") 2000, which is included in third-party products, such as

---

[3] The waiver requests and the proposed adjustment methodology should also be applied to any CLEC-specific calculations, including calculations related to the Individual Rule for Critical Measures. The CLEC-specific information in Exhibit 2 has been adjusted pursuant to the methodology set forth in Section III, *infra*.

[4] A port is a special purpose memory location to which communications messages are written and read.

VisualStudio.Net, Asp.net, Microsoft Access and others. The Slammer Worm, itself, is file-less and resides only in memory. It does not create or delete files, but actively scans for other vulnerable servers. It was this aggressive scanning and propagating that created enormous network and Internet traffic.

The Slammer Worm hit the national (and international) network quickly and without warning. Although most firms do not speak publicly about their security programs and breaches, industry analysts estimate that 200,000 devices were affected. Verizon was affected as were many other corporations and carriers, and the Internet, itself. Industry and press reports indicate that major corporations, such as Bank of America, the Canadian Imperial Bank of Commerce, Boeing, and J.P. Morgan Chase also were affected, as were telecommunications providers, such as AT&T, WorldCom, China Telecom and BellSouth. One of the most telling reports, however, came from Microsoft, which was infected and affected by the Slammer Worm. As Rick Devenuti, Microsoft's chief information officer stated in an interview on Monday, January 27, 2003, "[W]e are not sure how the virus got into our network… . It just takes one machine to get it going" (CNET News. com, **"**Microsoft Fails Slammer's Security Test", January 27, 2003).

B. EFFECT ON VERIZON'S SYSTEMS AND VERIZON'S RESPONSE

At 1:00 AM EST Saturday, January 25, 2003, Verizon Network Management detected network flooding. Verizon Network and Information Security teams immediately convened and began trouble-shooting the incident. Soon thereafter, the technical teams had identified traffic on what is known as the "1434 port" as the source of the traffic generation and began defensive actions to isolate and block port 1434 traffic on routers and firewalls. The internal data networks were isolated and quarantined into segments (North, Mid-Atlantic and West).

Later that morning, Verizon observed that its connections to the Internet were becoming flooded with very high utilization. This was highly irregular and gave Verizon technical teams evidence that Verizon was being attacked from the Internet. Given this alarming situation, and without the benefit of clear information from industry or government on the precise nature of the attack, Verizon determined that an external quarantine process was necessary to ensure the safety of its own and its partners' networks and systems. At that time, the wholesale interfaces (Corba, EDI, LSI (aka WEB GUI), EBI) were brought down to speed isolation and recovery from the infection. Verizon provided contemporaneous notification to CLECs of this event through normal communication channels (e-mail) on January 25, 2003. Because the Internet was still congested by the Slammer Worm, Verizon also notified by telephone the one CLEC that was attempting to exchange transactions with Verizon at that time. Verizon subsequently issued an updated bulletin with projected interface restoral times via the standard e-mail notification at approximately 10:00 PM, on Saturday, January 25, 2003.

From early morning Saturday, January 25, 2003, through late afternoon Sunday, January 26, 2003, Verizon proceeded to meticulously inspect, identify and remove infected devices, and where appropriate patch, test, and reconnect devices, thus incrementally restoring network segments. By 6:00 PM EST Sunday, January 26, 2003, internal networks and external interfaces were restored to business as usual.[5]

The attack, which affected many other large businesses and telecommunications carriers, had an impact on Verizon's operations, and created a situation that was beyond Verizon's control. In

[5] The FBI's National Infrastructure Protection Center has not yet identified who might be responsible for the release of the Slammer Worm.

particular, the downtime required to effect and assure a thorough recovery had an adverse impact on many elements of Verizon's business operations that utilize the internal data network and OSS and, therefore, on wholesale pre-order metrics that measure the performance of these business functions. Directly affected were the performance measures for OSS Interface Availability,[6] as Verizon proactively and defensively removed the interfaces from operation during prime time hours on Saturday, January 25, 2003, to aid in problem isolation and corrective action. As known by information security experts, this approach (blocking and monitoring network ingress and egress points) helps pinpoint compromised hosts and limit denial-of-service conditions based on bandwidth utilization.

Due to the network congestion caused by the Slammer Worm, individuals and systems attempting to perform transactions across the network were also affected. Dial tone service for Verizon retail and the CLECs purchasing services from Verizon was not affected.

C. VERIZON'S COMPUTER SECURITY PRACTICES

Verizon's computer security practices in the past have detected and helped mitigate the effects of other malicious virus or worm attacks. These practices enabled Verizon to quickly detect the Slammer Worm and begin defensive and recovery activities. In fact, Verizon was the first telecommunications company to report the incident to the National Communications Center – Information Sharing and Analysis Center ("NCC-ISAC"), an industry/government organization whose membership includes the major telecommunications carriers and the National Communications System. According to industry reports, the Slammer Worm "open[ed] a new era of fast-spreading viruses on the Internet… [it] doubled in size every 8.5 seconds when it first appeared…" compared to the Code Red

[6] The OSS Interface Availability metrics are the PO-2-02 metrics in the PAP and Carrier-to-Carrier Guidelines.

worm in 2001 which doubled in size every 37 minutes (CNET News.com, "Week in Review: Worm's Wrath", Feb. 7, 2003).

Verizon has an extensive security network in place to protect both its physical plant and its cyber assets, and one of the security practices employed by Verizon is participation in industry and government security information-sharing forums, such as the NCC-ISAC and the Computer Emergency Response Team Coordination Center at Carnegie Mellon University. Verizon also has engaged the services of a third-party firm specializing in software security, which proactively notifies Verizon of impending cyber attacks. None of these external groups provided Verizon with advance warning of the Slammer Worm.

Verizon's normal practices of maintaining the software infrastructure also include the process for obtaining, evaluating, testing and then deploying "fixes" or improvements to software components across its various systems. This is not a trivial function. When a security vulnerability or other software defect is discovered either by the supplier of a software component or users of the software, the software supplier undertakes the development of a "fix" for the defect. At the discretion of the supplier, the fix may be released to users either as part of a package of changes in a new software version or upgrade or may be released as a discrete repair to be applied to an existing version of the software. A discrete repair is also known as a "patch." Given the large amount of software in Verizon's computing infrastructure and the frequency with which patches and upgrades are released by vendors, patch management is a complex and time-consuming function.

Because application of a patch for a specific problem, such as a security vulnerability, can adversely impact the operation of other functions or software components within a specific system or application, testing of patches is normally prudent. In fact, a rush to install a patch that has not had a

significant amount of interoperability testing and broad-based user experience can result in unexpected consequences, since the patch may be later revoked by the supplier as ineffective or damaging, and may be superceded by a subsequent patch. Further, a security patch for a given software component may require, as a pre-condition to deployment, the installation of prior patches or intermediate releases having nothing at all to do with security, and/or it may require the installation or upgrade of a companion software component (for example, a given version of MS SQL Server will require a given version of Windows NT). Finally, the downtime associated with the application of a specific patch (and any related upgrade or other patches) can be substantial and must be efficiently managed, especially in a business such as Verizon's with thousands of systems, and the large number of wholesale customers that interface with Verizon's systems. Because of the complex interdependence between various patches and software release levels, the possibility of an adverse impact on the target system, downtime and a number of other factors, patch management represents a very serious challenge for most large businesses. Unfortunately, this already substantial challenge increases exponentially when a supplier issues "patches," even security patches, on a frequent basis. As Microsoft's CIO Devenuti stated in his January 27, 2003 interview, "At any given point in time, it is hard to be 100% patched with any machine."

Unfortunately, when the Slammer Worm hit, there were servers in Verizon and many other organizations and corporations that had not yet received a patch to fend off the Slammer Worm, which attacked a security vulnerability in MS SQL Server 2000 and MSDE 2000. In fact, many media accounts about the Slammer Worm described the challenges of patch management and Verizon's experience was fairly typical of the way many large businesses were affected. While Microsoft had released security patches that addressed the specific vulnerability exploited by the Slammer Worm, it is

only in hindsight that the specific patches to address the problem can be identified. In just the past 12 months alone, Microsoft has released 72 security patches to its various products. Among the latest was a patch issued in December 2002 for a vulnerability in its Windows NT 4.0, Windows 2000 and Windows XP products. This patch, however, was recently revoked on February 3, 2003 when it was determined that the patch for NT 4.0 machines would, under certain configurations, cause the operating system to fail. Moreover, recently Microsoft has released new patches for the Slammer Worm which it believes are much more user friendly than those originally released.

II. VERIZON MA IS ENTITLED TO A WAIVER FOR PERFORMANCE ON THREE PRE-ORDER MEASURES WITH ABSOLUTE STANDARDS DURING JANUARY 2003 DUE TO THE SLAMMER WORM

A. THE PAP STANDARD

Section II(J) of the PAP provides that:

> C2C service quality data may be influenced by factors beyond Verizon MA's control, Verizon MA may file Exception or Waiver petitions with the Department seeking to have the monthly service quality results modified on three generic grounds… .
>
> The third ground…relates to situations beyond Verizon MA's control that negatively affect its ability to satisfy only those measures with absolute standards. The performance requirements dictated by absolute standards establish the quality of service under normal operating conditions, and do not necessarily establish the level of performance to be achieved during periods of emergency, catastrophe, natural disaster, severe storms, work stoppage, or other events beyond Verizon MA's control… .

(PAP at 21&22; *see also* Appendix D (procedural schedule).)

While the PAP has been in existence in Massachusetts since April 2001, the PAP has been in existence in New York since January 2000, and the New York Public Service Commission ("NY PSC") has recognized that events beyond Verizon's control entitle Verizon New York ("Verizon NY")

to waivers of the PAP's service quality standards. The NY PSC granted Verizon NY waivers of certain monthly service performance after a work stoppage in August 2000.[7]

The Slammer Worm is an event similar to that waiverable event. It was an event beyond Verizon's control "that negatively affect[ed] its ability to satisfy . . . those measures with absolute standards." The Slammer Worm struck Verizon and numerous other companies that rely on Microsoft products without warning in the early hours of January 25, 2003. Verizon worked around-the-clock to resolve the problems the Slammer Worm created. Prior to the Slammer Worm attack, Verizon took reasonable precautions to protect its computer systems from attack. In fact, Verizon's detection, isolation and recovery from the attack in approximately 40 hours was made possible by Verizon's ongoing business practices and its management of a secure, heterogeneous and complex computing infrastructure. Verizon's use of secure access infrastructure utilizing firewalls, ongoing security vigilance to detect and repudiate attacks, 24x7 network traffic monitoring, and 24x7 network device, server and system availability monitoring for critical systems allowed Verizon to restore functions and operations incrementally and fully emerge from the crisis by Sunday night. The Slammer Worm and other malicious incidents demonstrate the inherent vulnerability of shared and interconnected data networks. The collective information technology industry, including Verizon's Information Technology organization, and the government continue to work together to further protect and secure this shared resource.

---

[7] Case 99-C-0949, et al., Petition of Bell Atlantic - New York for Approval of a Performance Assurance Plan and Change Control Assurance Plan, filed in C 97-C-0271, "Order Granting in Part and Denying in Part Requests for Waivers of Service Quality Targets" (issued June 7, 2001) ("The Commission finds that the August work stoppage was an extraordinary event beyond the control of Verizon justifying the granting of waivers from the service quality requirements of the PAP"). Although the PAP has been in effect in New York since January 2000, the work stoppage waivers are the only waivers Verizon has requested under the PAP. After the September 11, 2001 terrorist attacks, the NY PSC, *sua sponte*, suspended the operation of the PAP for three months. To date, PAP waiver requests have not been filed with any other state commissions.

Some parties may argue that Verizon MA should not be granted the waiver because it should have had patches in place to prevent the Slammer Worm from infecting its systems. Any such arguments should be rejected. The threshold question is not whether Microsoft patches existed to prevent the Slammer Worm from infecting Microsoft systems, but whether Verizon exercised reasonable, prudent judgment, consistent with industry practices, in operating and protecting its cyber facilities.[8] The PAP states that Verizon must demonstrate "why Verizon MA's normal reasonable preparations for difficult situations proved inadequate…" (PAP at 23). Verizon MA has made that showing.

Indeed, the record demonstrates that Verizon acted in a prudent, reasonable manner. As outlined above, Verizon has sophisticated and extensive procedures for the operation and protection of its cyber facilities, including the OSS available for CLECs. Moreover, patch management is an extremely complex task. Many other well-respected and well-run companies were also infected by the Slammer Worm and Verizon's experience appears to have been typical of these companies. Verizon operated and protected its system in a reasonable fashion, similar to other large corporations. In fact, in

---

[8] *See*, *e.g.*, D.T.E. 02-24/25, Petition of Fitchburg Gas and Electric Light Company, pursuant to General Laws Chapter 164, § 94, and 220 C.M.R. §§ 5.00 et seq. for a General Increase in Gas and Electric Rates, 2002 Mass. PUC LEXIS 59, at *53 (December 2, 2002 ("[a] prudence review involves a determination of whether the utility's actions, based on all that the utility knew or should have known at the time, were reasonable and prudent in light of the extant circumstances. Such a determination may not properly be made on the basis of *hindsight* judgments, nor is it appropriate for the Department merely to substitute its own judgment for the judgments made by the management of the utility.") (emphasis added); *see also* Case 27563, Long Island Lighting Company - Phase II - Proceeding on Motion of the Commission to Investigate the Cost of Construction of the Shoreham Nuclear Generating Facility, "Opinion and Order Determining Prudent Costs," Opinion No. 85-23 (issued December 16, 1985) ("[T]he company's conduct should be judged by asking whether the conduct was reasonable at the time, under all the circumstances, considering that the company had to solve its problems prospectively rather than in reliance on hindsight. In effect, our responsibility is to determine how reasonable people would have performed the task that confronted the company.'") (emphasis added) (footnotes and citations omitted); *see also* Philadelphia Electric Co. v. Pennsylvania Public Utility Com., 114 Pa. Commw. 22, 538 A.2d 98 (1988*), affirmed in part and reversed in part*, 522 Pa.

(continued . . .)

determining whether Verizon's actions in defending its systems from being infected by the Slammer Worm were reasonable, the Department need look no further than Microsoft, the developer of the infected systems and the associated security patches. The fact that Microsoft, itself, was infected by the Slammer Worm speaks volumes about the difficulties of being "100% patched" at all times.

In the days following the Slammer Worm attack, the press included a number of articles addressing the challenges related to patch management, and a number of security experts opined on the difficulties of patch management. For example, Bruce Schneier, chief technology officer for network protection firm Counterpane Internet Security stated "[The Slammer Worm] shows that the notion of patching doesn't work. Publicly, they [Microsoft] are saying it's not our fault, because you should have patched. But Microsoft's own actions show that you can't reasonably expect people to be able to keep up with patches" (CNET News.com, "Microsoft Fails Slammer's Security Test," by Robert Lemos, Jan. 27, 2003). Mr. Schneier, also pointed out that "numerous software patches are released every week. Systems managers are thus expected 'to patch their systems about once a day, for ever'. This is unrealistic. And even if most systems are patched, an unpatched minority can wreak havoc" (The Economist (US) Feb1, 2003 v366). One article noted that "Microsoft released a service pack that would have fixed the problems the week before Slammer hit. But not only are there too many patches to keep up with, people are reluctant to install them for fear they will interfere with their systems. Microsoft admits making a mistake with the SQL fix and has 'egg on our face' over being hit by the worm, . . . 'What this demonstrates and what we [Microsoft] readily acknowledge is the patch

---

(. . . continued)

338, 561 A.2d 1224 (1989).

management process is too complex'. . . . 'Microsoft is committed to reorganizing [its] patch system and delivering high-quality patches in a streamlined way'" (CNN.com, "Experts: Microsoft Security Gets an 'F'," February 1, 2003). *See also* CNETNews.com, *supra*, "Week in Review: Worm's Wrath." ("The worm's most significant casualty may be the perception that companies can remain secure by keeping up with software patches and other protective updates. Instead, security experts say, companies need to begin treating such attacks as inevitable and focus on limiting their damage, rather than expending every effort trying to create an ironclad perimeter.")

In short, Verizon acted reasonably under the circumstances. Thus, the Department should grant Verizon MA a waiver of the absolute service standards that Verizon could not satisfy as a result of the Slammer Worm.

B. THE PO-2-02 METRICS

For the purposes of this waiver, Verizon MA has identified three specific measures with absolute standards that the Department should waive: (1) PO-2-02-6020 "OSS Interface Availability – Prime – EDI"; (2) PO-2-02-6030 OSS Interface Availability – Prime – Corba"; and (3) PO-2-02-6080 "OSS Interface Availability – Prime – Web GUI." These measures, which measure activity in prime time (6:00 AM to 12:00 AM EST Monday through Saturday, (excluding major holidays)) have a standard of equal to or greater than 99.5%. Each measure is included in the UNE and Resale MOEs of the PAP, as well as in Critical Measure No. 1.

As demonstrated in the tables below, prior to the Slammer Worm attack, Verizon MA satisfied each of these measures on a regular, monthly basis.

Performance on PO-2-02 Metrics

Eight Month View (%)

	June	July	Aug	Sept	Oct	Nov	Dec	Jan
PO-2-02-6020 (EDI)	100	100	99.89	100	99.96	99.89	100	97.44
PO-2-02-6030 (Corba)	100	100	99.97	100	100	99.98	100	98.65
PO-2-02-6080 (Web GUI)	99.75	100	99.75	100	99.76	99.80	100	96.92

But for the Slammer Worm, Verizon MA would have been able to provide satisfactory service on these measures. As noted above, the interfaces, including EDI and Corba, were brought down Saturday to speed the isolation and recovery from the Slammer Worm. In addition, the Web GUI, which operates via the Internet, was affected by the Internet flooding that the Slammer Worm caused. Accordingly, the Department should waive the service quality results recorded under the PO-2-02 measures and allow Verizon MA to adjust the service quality results for these measures using the process outlined below.

III. THE MONTHLY DATA SHOULD BE ADJUSTED BY EXCLUDING THE AFFECTED TIME PERIOD

The PAP is silent on how the service data affected by an abnormal event should be treated in calculating a revised monthly report. For example, there is no indication whether the affected data should be excluded completely from the report or whether a normalization methodology should be used to adjust the data. A normalization methodology would take out the influence of the Slammer Worm on the data and use the adjusted data along with the unadjusted data for the remaining measures to

calculate the amount of bill credits due to CLECs under the PAP. This is the methodology that Verizon NY proposed be used for that state for the August 2000 Work Stoppage Waivers. In that case, the abnormal event occurred over numerous days. Here, only the performance on one day, Saturday January 25, 2003, is relevant to the calculation of the monthly data for the affected metrics.[9] A more appropriate method in this case would be to exclude the affected day. Accordingly, Verizon MA proposes that Saturday, January 25, 2003, be excluded from the calculation of the PO-2-02 metrics for the January performance month, and the reports annexed as part of Exhibit 2 reflect these exclusions.

IV. NO PARITY MEASURES WERE ADVERSELY AFFECTED BY THE SLAMMER WORM

The PAP provides that "this waiver process shall not be available for those metrics for which Verizon MA's wholesale performance is measured by comparison to retail performance (parity metrics)" (PAP at 23). The PAP, however, requires Verizon MA to "include an analysis of the extent to which the parity metrics (retail and wholesale) were affected by the subject event…" (*Id*.). In this case, the Slammer Worm attack did not prevent Verizon MA from providing parity service to the CLECs. In fact, Verizon MA has been providing excellent service to its wholesale customers.

[9] The Slammer Worm also affected Sunday, January 26, 2003, but Sunday is not a prime time day and is not covered by the PO-2-02 metrics.

V. CONCLUSION

Despite its best efforts, Verizon MA was unable due to the Slammer Worm to satisfy the service quality standards for the PO-2-02 metrics in the PAP for January 2003. Accordingly, Verizon MA should be granted a waiver for the performance on the PO-2-02 metrics.

Respectfully submitted,

VERIZON MASSACHUSETTS

Bruce P. Beausejour
185 Franklin Street, 13th Floor
Boston, Massachusetts 02110-1585
(617) 743-2445

Dated: March 18, 2003